UNIVERSIDAD COMPLUTENSE
MADRID

AVISO DE CONFERENCIA

Tu corazón podría ser hackeado: Seguridad en Dispositivos Médicos Implantables

Prof. Pedro Peris López

Universidad Carlos III de Madrid

Facultad de Informática
Sala de Grados • 20 de mayo de 2013 • 16:00
entrada libre hasta completar el aforo

resumen:

Un número cada vez mayor de dispositivos médicos implantables, IMDs (de sus siglas en inglés, Implantable Medical Devices), estarán disponibles en un futuro no muy lejano debido a los continuos avances en el campo de la bioingeniería. La primera generación de IMDs era ya capaz de controlar diferentes condiciones fisiológicas en el cuerpo, ayudando a tratar una amplia gama de dolencias tales como arritmias cardiacas, diabetes, párkinson, etc. En la actualidad, la segunda generación de IMDs ha irrumpido con fuerza en el mercado y está siendo implantada en nuestros hospitales. Estos nuevos dispositivos basan una parte de su funcionalidad en la comunicación a distancia con una estación base, permitiendo la realización de tareas de diagnostico, terapia e incluso actualización de manera remota. La nueva capacidad de comunicación inalámbrica expone al IMD a entornos abiertos que no se habían considerado anteriormente. Estudios recientes han demostrado que dicha conectividad puede ser explotada para por ejemplo comprometer la confidencialidad de los datos transmitidos por el IMD (información confidencial del paciente) o suplantar a las entidades autorizadas con el fin de comunicarse con el dispositivo (un atacante podría reprogramar el IMD cambiado o interrumpiendo terapias y en caso más dramático inducirles un fallo fisiológico). A pesar de estas amenazas de seguridad, existen numerosos IMDs que carecen de mecanismos de seguridad adecuados, tales como protocolos de autenticación o cifrado de los datos. Los problemas de privacidad, fugas de información confidencial y accesos no autorizados, introducen metas de seguridad nuevas en el campo. Sin embargo, aunque se conocen los riegos, proveer de mecanismos de seguridad así como proteger la información no son tareas triviales, ya que soluciones clásicas utilizadas en otras áreas no son validas en este caso. Una de las cuestiones clave es la existencia de tensiones fundamentales entre los objetivos de privacidad/seguridad y la seguridad física del paciente.

Sobre Pedro Peris:

PEDRO PERIS LÓPEZ es Ingeniero de Telecomunicación (2004) y Doctor en Ciencia y Tecnología Informática (2010) por la Universidad Carlos III de Madrid. Durante el periodo comprendido entre octubre del 2004 y septiembre del 2009 fue Profesor ayudante en la Universidad Carlos III de Madrid realizando tanto tareas docentes como de investigación. En enero de 2009 se incorporó, como investigador posdoctoral, a la Delft University of Technology. Entre Septiembre del 2010 y Septiembre de 2011 compaginó su actividad de investigación en la Universidad de Delft con la de profesor asociado en la Universidad Carlos III donde imparte un día a la semana cursos de grado y máster. Desde Septiembre de 2011 es profesor Visitante de la Universidad Carlos III de Madrid (COSEC Lab). Ha publicado números trabajos en conferencias (29) internacionales con proceso de revisión por pares y revistas (21) de reconocido prestigio con índice de impacto. A su vez, ha contribuido en diferentes capítulos de libros (5) y publicado un libro sobre criptografía ligera y dispositivos de identificación por radiofrecuencia – área en la que puede ser considerado un experto. Tres de sus trabajos posen un número de citas superior a 150 y, en su totalidad, sus trabajos han sido citados en 1105 ocasiones. Pose un índice h de 14 y su índice g es de 31 (Consultado 08/03/2013).

Ha sido invitado como conferenciante en Universidades (ej. Radboud University Nijmegen, K.U.Leuven, etc.) y centros de Investigación (ej. I2R Singapore). Ha sido miembro del comité de programa en reconocidas conferencias internacionales – incluyendo algunas de las mas relevantes en su área de investigación, ej. RFIDsec Asia, RFIDSec, IEEE RFID. A su vez, actúa como revisor en numerosas y prestigiosas revistas internacionales y sirve como editor asociado en Journal of Engineering (Hindawi Publishing Corporation) y Journal of Security & Communication Networks (John Wiley & Sons, Ltd). Ha participado en números proyectos de I+D+I tanto nacionales como internacionales. En la actualidad se encuentra vinculado al proyecto SACO (Simulador Avanzado para la Ciberdefensa Organizada) y participa en la acción COST (IC 1204). Finalmente, cabe mencionar que sirve como evaluador de proyectos en Fund for Scientific Research - FNRS (Belgium) y Austrian Science Fund FWF.